RFC 5448bis
EAP-AKA’ Update

Jari Arkko, Vesa Lehtovirta, Vesa Torvinen
Ericsson Research
(+ RFC 5448 author Pasi Eronen)

draft-ietf-emu-rfc5448bis-01.txt

Background

EAP-AKA (RFC 4187) & revised EAP-AKA’ (RFC 5448)

These have been very widely implemented, somewhat widely used for WLAN access authentication

- 2/3/4G access uses native SIM card and AKA, not EAP
- 5G access authentication introduces the use of EAP for 5G access

The Update

- Updates are bugs in the current specification, missed items or security considerations, or specifying behaviour for new situations introduced in 5G
    - Network name bindings specified for 5G
    - Identifier usage specified for 5G
    - Include a definition of exported parameters as required by RFC 5247
    - References updated to newer 3GPP and NIST specifications

Identifier Usage

- Previously this was clear for all cases — use the name that was sent; clarity is important since identifiers are used in KDF
- With 5G, this changes for two reasons:
    - The EAP session is inside the native 5G network attachment procedure which does not use EAP identity request & response
    - In 5G, there are two distinct identifiers for users, the permanent, private one (SUPI) which is never sent, and a temporary one that can be sent over the wire (SUCI)
- When network name begins with 5G, use SUPI for key generation; otherwise behave exactly as RFC 5448 specified

Version -00

- Simply introduced the document as WG document

Version -01

- Updates relationship to RFC 4187
- Clarifies language relating to obsoleting RFC 5448
- Updates several references to newer ones
- Specifies what identifiers should be used in key derivation formula in 5G
- Specifies how to construct the network name in 5G

Next Steps

- Give us feedback & discuss!
- Ongoing coordination with 3GPP, but we believe this version of draft is in sync with current 3GPP Release 15 specifications
- Proceed?